UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF TEXAS

PATRICIA DEAN individually and on behalf of all similarly situated persons,

Plaintiff,

v.

AT&T, INC.,

Defendant.

Case No. 3:24-cv-00776

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Patricia Dean ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant AT&T, INC. ("AT&T"), a Texas corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of a recent targeted cyberattack and data breach ("Data Breach") in which AT&T, the largest telecommunications services company in the United States, lost control over more than 73 million customers' personal data and other sensitive information. Those customers, including Plaintiffs and Class Members, suffered ascertainable losses from this Data Breach including the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

2. Plaintiff's and Class Members' personal data and other sensitive information—

which was entrusted to Defendant for safe keeping—was compromised and unlawfully accessed due to the Data Breach.

3. The Data Breach included personally identifiable information ("PII") that Defendant collected and maintained. Information compromised in the Data Breach includes, *inter alia*, names, addresses, phone numbers, dates of birth, Social Security Numbers, and email addresses ("Private Information").

4. Plaintiff brings this class action lawsuit to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their information had been subject to the unauthorized access of unknown third parties and precisely what specific type of information was accessed.

5. Defendant collected and shared Private Information in a reckless manner.

6. In particular, Private Information was collected by Defendant, inadequately secured, and shared with a vendor who had insufficient cybersecurity protections in place to protect that Private Information.

7. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. Plaintiff's and Class Members' identities are now at increased risk of identity theft because of Defendant's negligent conduct since the Private Information that Defendant collected and promised to protect is now in the hands of data thieves.

9. Armed with the Private Information accessed in the Data Breach, data thieves can

commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

11. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security protocols, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

14. Plaintiff Patricia Dean is, and at all times mentioned herein was, an individual citizen of the State of Illinois. Plaintiff Dean is an AT&T customer and received telecommunication services from AT&T.

15. Defendant AT&T is a telecommunications company that provides, among other things, wireless network services, cellular data plans, cell phone plans, and Internet connection

plans.

16. Defendant is headquartered at 208 South Akard Street Dallas, Texas 75202, and may be served via their registered agent CT Corporation System, 1999 Bryan Street., Ste. 900, Dallas, Texas 75201.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

18. This Court has personal jurisdiction over Defendant AT&T because Defendant is headquartered in Texas and has thus availed itself of the rights and benefits of the State of Texas by engaging in activities including (i) directly and/or through its parent companies, affiliates and/or agents providing services throughout the United States in this judicial district and abroad; (ii) conducting substantial business in this forum; (iii) having a registered agent to accept service of process in the State of Texas; and/or (iv) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in Texas and in this judicial District.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the Northern District of Texas.

DEFENDANT AT&T'S BUSINESS

20. Defendant AT&T is a company that provides telecommunications services across the United States.

21. In the ordinary course of providing telecommunications services, customers must provide to AT&T access to certain Private Information. AT&T specifies the following types of personal data collected in its Privacy Notice:

> **The information we collect**
>
> To better run our business, we collect information about you, your equipment and how you use our products and services. This can include:
>
> - **Account information.** You give us information about yourself, such as contact and billing information. We also keep service-related history and details, including Customer Proprietary Network Information.
> - **Equipment information.** We collect information about equipment on our network like the type of device you use, device ID, and phone number.
> - **Network performance.** We monitor and test the health and performance of our network. This includes your use of Products and Services to show how our network and your device are working.
> - **Location information.** Location data is automatically generated when devices, products and services interact with cell towers and Wi-Fi routers. Location can also be generated by Bluetooth services, network devices and other tech, including GPS satellites.
> - **Web browsing and app information.** We automatically collect a variety of information which may include time spent on websites or apps, website and IP addresses and advertising IDs. It also can include links and ads seen, videos watched, search terms entered and items placed in online AT&T shopping carts. We may use pixels, cookies and similar tools to collect this information. We don't decrypt information from secure websites or apps – such as passwords or banking information.
> - **Biometric information.** Fingerprints, voice prints and face scans are examples of biological characteristics that may be used to identify individuals. Learn more in our Biometric Information Privacy Notice.
> - **Third-party information.** We get information from outside sources like credit reports, marketing mailing lists and commercially available demographic and geographic data. Social media posts also may be collected, if you reach out to us directly or mention AT&T.
>
> All these types of information are considered Personal Information when they can reasonably be linked to you as an identifiable person or household. For instance,

> information is personal when it can be linked to your name, account number or device.[1]

22. Within AT&T's Privacy Notice, AT&T states the following about keeping Private Information private and secure:

> Thank you for reading our Privacy Notice. *Your privacy is important to you and to us*.
> …
> This notice applies to AT&T products and services including internet, wireless, voice and AT&T apps.
> …
> **Your privacy choices and controls**
> You can manage how we use and share your information for certain activities including advertising and marketing. Here are key examples:
>
> **Do not sell or share my personal information.** We may share information with other companies in limited ways, such as exchanging subscriber lists for joint marketing.
> …
> **Data retention and security**
> We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.
>
> *No security measures are perfect. We can't guarantee that your information will never be disclosed in a manner inconsistent with this notice. If a breach occurs, we'll notify you as required by law*.[2]

23. Thus, because of the highly sensitive and personal nature of the information it acquires, AT&T promises in its Privacy Notice to, among other things, maintain the privacy and security of Private Information.

24. As a condition of receiving telecommunications services, Defendant requires that

[1] *AT&T Privacy Notice*, AT&T, Inc., https://about.att.com/privacy/privacy-notice.html (last accessed Mar. 28, 2024).
[2] *Id*.

its customers entrust it with highly sensitive personal information.

25. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

26. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

27. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

THE DATA BREACH

A. 2021 Stealing of Database ("2021 Data Incident")

28. On or about August 19, 2021, a criminal hacking group called "ShinyHunters" began selling on a hacking forum a database which, according to ShinyHunters, contains Personal Customer Data of over 70 million AT&T customers.[3]

29. While attempting to sell the database, ShinyHunters only revealed sample data from the compromised database, which included customers' names, addresses, phone numbers, Social Security numbers, and dates of birth.[4]

30. AT&T maintained, without providing any evidence, that the data samples leaked from the compromised database did not come from AT&T's systems and that AT&T had not been

[3] *AT&T denies data breach after hacker auctions 70 million user database*, BleepingComputer (Aug. 20, 2021), https://www.bleepingcomputer.com/news/security/atandt-denies-data-breach-after-hacker-auctions-70-million-user-database/
[4] *Id*.

breached.[5]

31. AT&T also did not confirm whether the leaked data came from a breach of a third-party partner's information technology systems which may have held Private Information.[6]

32. ShinyHunters challenged AT&T's denials of the Data Breach coming from AT&T or one of its third-party partners, stating "I don't care if they don't admit. I'm just selling."[7]

33. ShinyHunters also stated that the criminal group was willing to "negotiate" with AT&T.[8]

34. Shortly after the 2021 Data Incident, a security researcher reported that two of the four individuals in the data samples leaked by ShinyHunters were confirmed to have accounts on att.com.[9]

35. AT&T did not notify any of its customers, including Plaintiff and Class Members, of the 2021 Data Incident.

B. 2024 Leak of Private Information ("2024 Data Incident")

36. On or about March 17, 2024, another cybercrime actor known as "MajorNelson" posted on an Internet forum the entire dataset of the stolen database from the 2021 Data Incident, the database of which ShinyHunters attempted to sell.[10]

37. The data leaked by MajorNelson included the following data types from approximately 73 million individuals, *inter alia*: names, addresses, phone numbers, dates of birth,

[5] *Id*.
[6] *Id*.
[7] *Id*.
[8] *Id*.
[9] *Id*.
[10] *AT&T says leaked data of 70 million people is not from its systems*, BleepingComputer (Mar. 17, 2024), https://www.bleepingcomputer.com/news/security/att-says-leaked-data-of-70-million-people-is-not-from-its-systems/amp/.

and Social Security numbers.[11]

38. On March 19, 2024, Troy Hunt—a security researcher and the creator of the data breach notification website "Have I Been Pwned"—posted on his blog about the AT&T Data Breach.[12]

39. In the blog post, Mr. Hunt concluded that the leaked data from the Data Breach was authentic after he spoke with several "Have I Been Pwned" subscribers who were AT&T customers and who confirmed the accuracy of the leaked data.[13]

40. Moreover, Mr. Hunt noted that the Internet forum on which the leaked data was posted is not on the 'dark web,' but rather on the traditional Web "easily accessed by a normal web browser."[14]

41. The 2021 Data Incident combined with the 2024 Data Incident (together, the "Data Breach") caused significant harm to Plaintiff and Class Members.

C. AT&T Failed to Safeguard Plaintiff's and Class Members' Private Information

42. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

43. Plaintiff and Class Members provided their Private Information to AT&T with the reasonable expectation and mutual understanding that Private Information would comply with

[11] *Id*.
[12] Troy Hunt, *Inside the Massive Alleged AT&T Data Breach*, TroyHunt.com (Mar. 19, 2024), https://www.troyhunt.com/inside-the-massive-alleged-att-data-breach/.
[13] *Id*.
[14] *Id*. ("As I'm fond of saying, there's only one thing worse than your data appearing on the dark web: it's appearing on the clear web. And that's precisely where it is; the forum [the leaked data] was posted to isn't within the shady underbelly of a Tor hidden service, it's out there in plain sight on a public forum easily accessed by a normal web browser.")

their obligations to keep such information confidential and secure from unauthorized access.

44. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the breach.

45. In light of recent high profile data breaches at other companies, Defendant knew or should have known that electronic records would be targeted by cybercriminals.

46. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[15]

47. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

48. AT&T failed to implement adequate data security measures to safeguard Plaintiff's and Class Members' Private Information as evidenced by the database stolen by ShinyHunters in 2021 and by the full leak of about 73 million individuals' Private Information by MajorNelson in 2024, nearly three years after the 2021 Data Incident.

49. Despite the first Data Incident having occurred in August 2021 (and again on March 2024), AT&T has made no effort to notify the public about the severity of the Data Breach nor has AT&T given to potential victims of the Data Breach instructions on how to keep their Private Information safe.

50. Even though the Private Information at issue has been compromised and leaked for

[15] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Jan. 5, 2023).

about two and a half years, AT&T has done nothing to get that leaked Private Information taken down from places where the Private Information should not be, such as in the aforementioned Internet *fora*, which are on the Clear Web.

51. Further, AT&T has not done anything to determine the source of the Data Breach. This is evidenced by AT&T's reluctance to confirm whether the Data Breach may be attributed to a third-party partner to whom AT&T entrusted the processing and safekeeping of a substantial amount of Plaintiff's and Class Members' Private Information.

52. Considering that the Data Breach likely occurred as a result of malicious actors—such as ShinyHunter and MajorNelson—exploiting a data security weakness in one of AT&T's third-party processors of Private Information, AT&T failed to adequately verify the adequacy of security measures, if any, that such third-party processors had in place meant to protect the Private Information.

D. Defendant Failed to Comply with FTC Guidelines

53. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

54. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security

problems.[16] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[17]

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

56. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Private Information is an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

58. Defendant was at all times fully aware of its obligation to protect the Private

[16] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 5, 2023).
[17] *Id.*

Information of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Failed to Comply with Industry Standards

59. As shown above, experts studying cyber security routinely identify companies as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

60. Several best practices have been identified that a minimum should be implemented by companies like Defendant, including but not limited to ensuring Private Information is only shared with third parties when reasonably necessary and that those vendors have appropriate cybersecurity systems and protocols in place.

61. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security ("CIS") released its Critical Security Controls ("CSC"), and all businesses are strongly advised to follow these actions. The CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[18]

62. Other best cybersecurity practices that are standard in the telecommunications industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security

[18] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Jan. 5, 2021).

systems; protection against any possible communication system; and training staff regarding critical points.

F. Cyberattacks and Data Breaches Put Individuals at an Increased Risk of Fraud and Identity Theft

63. Cyberattacks and data breaches on businesses are problematic because of the increased risk of fraud and identity theft.

64. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[19]

65. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

66. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit

[19] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited Jan. 5, 2024).

reports.[20]

67. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

68. Identity thieves can use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. Also, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

69. Moreover, theft of Private Information is also gravely serious. PII is a valuable property right.[21]

70. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

71. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information is stolen and when it is used.

72. According to the U.S. Government Accountability Office, which conducted a study

[20] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited January 5, 2024).

[21] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

73. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

74. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

75. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts and other types of accounts for many years to come.

76. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[22] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

77. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[23] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social

[22] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[23] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 5, 2024).

Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[24] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

78. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[25]

79. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[26]

80. Because of the value of its collected and stored data, the telecommunications industry has experienced disproportionally higher numbers of data theft events than other industries.

81. For this reason, Defendant knew or should have known about these dangers and

[24] *Id* at 4.
[25] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.
[26] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

strengthened its data protocols accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

G. Plaintiff's and Class Members' Damages

82. To date, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of Data Breach.

83. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

84. On or about March 30, 2024, Plaintiff Patricia Dean, a 20-year customer of AT&T, received an email from AT&T that her Private Information was involved in the Data Breach

85. Plaintiff Dean continued to research the data breach and learned that it involved 73 million AT&T customers' Private Information.

86. Plaintiff has since confirmed that her Private Information was indeed impacted in the Data Breach and that her Private Information is readily accessible via a search of the publicly available database containing AT&T customers' Private Information.

87. Plaintiff's Private Information was compromised as a direct and proximate result of the Data Breach.

88. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

89. As a result of the Data Breach, the Private Information of over 73 million AT&T customers, including Plaintiff Dean and Class Members, are available on the Internet for users, including criminals, to find, search through, and download.

90. As a direct and proximate result of Defendant's conduct, Plaintiff and Class

Members have been forced to expend time dealing with the effects of the Data Breach.

91. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

92. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

93. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

94. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

95. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to AT&T was intended to be used by AT&T to fund adequate security of Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for.

96. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse. Indeed, AT&T has not yet provided any instructions to Plaintiff and Class Members about all the time that they will need to spend monitor their own accounts, or about how to establish a security freeze on their

credit reports.

97. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled, and;

k. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

98. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from

further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

99. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

100. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

CLASS ALLEGATIONS

101. Plaintiff brings this Action as a class action under Federal Rule of Civil Procedure 23 and seeks certification of the following nationwide Class:

> Nationwide Class: All persons in the United States whose personal information was accessed, compromised, copied, stolen, and/or revealed as a result of Defendant AT&T, Inc.'s Data Breach.

102. Excluded from the Class are Defendant, its officers and directors, and Members of their immediate families or their legal representatives, heirs, successors or assigns and any entity in which Defendant has or had a controlling interest.

103. Class certification of Plaintiff's claims is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis utilizing the same evidence as would be used to prove those elements in separate actions alleging the same claims.

104. **Numerosity—Federal Rule of Civil Procedure 23(a)(1)**. The Members of the

Class are so numerous that joinder of all Class Members would be impracticable. Upon information and belief, the Class number is over 70 million. Also, the Class is comprised of an easily ascertainable set of AT&T customers who were impacted by the Data Breach. The exact number of Class Members can be confirmed through discovery, which includes Defendant's records. The resolution of Plaintiff's and Class Members' claims through a class action will behoove the Parties and this Court.

105. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3)**. Common questions of fact and law exist as to all Members of the Class and predominate over questions affecting only individual Class Members. These common questions of law or fact, include, among other things:

a. Whether Defendant's cybersecurity systems and/or protocols before and during the Data Breach complied with relevant data security laws and industry standards;

b. Whether Defendant properly implemented their purported security measures to safeguard Plaintiff's and Class Members' private information from unauthorized access, propagation, and misuse;

c. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first discovered the same;

d. Whether Defendant disclosed Plaintiff's and Class Members' Private Information in contravention of the understanding that the information was being revealed in confidence and should be maintained;

e. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures and security controls to preclude unauthorized

access to Plaintiff's and the Class Members' Private Information;

f. Whether Defendant was unjustly enriched by its actions; and

g. Whether Plaintiff and Class Members are entitled to damages, injunctive relief, or other equitable relief, and the extent of such damages and relief.

106. Defendant engaged in a common course of conduct granting rise to the legal rights sought to be enforced by Plaintiff, on behalf of hersel and other Members of the Class. Similar or identical common law violations, business practices, and injuries are involved.

107. **Typicality—Federal Rule of Civil Procedure 23(a)(3)**. Plaintiff's claims are typical of the claims of the other Members of the Class because, *inter alia*, all Class Members were similarly injured and sustained similar monetary and economic injuries as a result of Defendant's misconduct described herein and were accordingly subject to the alleged Data Breach. Also, there are no defenses available to Defendant that are unique to Plaintiff.

108. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4)**. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class he seeks to represent, he retained counsel competent and experienced in complex class action litigation, and he will prosecute this action earnestly. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

109. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2)**. Defendant acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate regarding the Class under Federal Rule of Civil Procedure 23(b)(2).

110. **Superiority—Federal Rule of Civil Procedure 23(b)(3)**. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class

action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

111. Class certification is also appropriate under Rules 23(b)(1) and/or (b)(2) because:

a. The prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications establishing conflicting standards of conduct for Defendant;

b. The prosecution of separate actions by individual Class Members would create a risk of adjudication that would be dispositive of the interests of other Class Members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests; and

c. Defendant has acted and refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief regarding the Members of the Class as a whole.

112. Class certification is also appropriate because this Court can designate specific claims or issues or class-wise treatment and may designate multiple subclasses under Federal Rule of Civil Procedure 23(c)(4).

113. No unusual difficulties are likely to be encountered in the management of this action as a class action.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

114. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-114 as if fully set forth herein. Plaintiff brings this claim individually and on behalf of the Class Members.

115. In order to receive telecommunications services, Defendant required Plaintiff and Class Members to submit non-public Private Information, such as PII.

116. Plaintiff and Class Members entrusted their Private Information to Defendant with the understanding that Defendant would safeguard their information.

117. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to fully vet vendors with whom it shared Private Information and ensure that those vendors had adequate data security protocols and procedures in place.

118. Defendant owed a nondelegable duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

119. Defendant's duty of care to use reasonable security measures arose as a result of

the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

120. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

121. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the law described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

122. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures in its own systems to protect Class Members' Private Information and by failing to properly verify that its third party processors implemented data security measures adequate to safeguard Plaintiff's and Class Member's Private Information.

123. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the telecommunications industry.

124. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

125. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

126. Plaintiff and Class Members are also entitled to injunctive relief requiring

Defendant to (i) strengthen its data security protocols and procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit and identity monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

127. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-114 as if fully set forth herein. Plaintiff brings this claim individually and on behalf of the Class Members.

128. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

129. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

130. Defendant breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws.

131. It was reasonably foreseeable, particularly given the growing number of data breaches of personal information in the telecommunications sector, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Plaintiff's and Class Members' Private Information.

132. Plaintiff's and Class Members' Private Information constitutes personal property

that was stolen due to Defendant's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

133. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Private Information and Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek damages and other relief as a result of Defendant's negligence.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

134. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-114 as if fully set forth herein. Plaintiff brings this claim individually and on behalf of the Class Members.

135. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of telecommunications services, as well as implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

136. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when he signed up with AT&T for telecommunications services.

137. The valid and enforceable implied contracts to provide telecommunications services that Plaintiff and Class Members entered into with Defendant include the promise to protect non-public Private Information given to Defendant or that Defendant creates on its own from disclosure.

138. When Plaintiff and Class Members provided their Private Information to Defendant

in exchange for telecommunications services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

139. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

140. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

141. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to ensure adequate data security. Defendant failed to do so.

142. Under the implied contracts, Defendant promised and were obligated to: (a) provide telecommunications services to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' Private Information. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

143. Both the provision of telecommunication services and the protection of Plaintiff's and Class Members' Private Information were material aspects of these implied contracts.

144. The implied contracts for the provision of telecommunications services – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

145. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual

obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

146. Customers of telecommunications services value their privacy, the privacy of their dependents, and the ability to keep their PII associated with obtaining telecommunications services private. To customers such as Plaintiff and Class Members, telecommunications services that do not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than the similar services that adhere to industry-standard data security. Plaintiff and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected or entrusted their Private Information to Defendant in the absence of its implied promise to adopt reasonable data security measures.

147. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant, and paid for the provided telecommunications services in exchange for, amongst other things, both the provision of telecommunications services and the protection of their Private Information.

148. Plaintiff and Class Members performed their obligations under the contract when they paid for their telecommunications services and provided their Private Information.

149. Defendant materially breached its contractual obligation to protect the non-public Private Information Defendant gathered when the sensitive information was accessed by unauthorized personnel as part of the cyberattacks and Data Breach.

150. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the

privacy of Plaintiff's and Class Members' Private Information as evidenced by its repeated unauthorized disclosures of Private Information to at least two cybercriminal actors—ShinyHunters and MajorNelson. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

151. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

152. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received telecommunications services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the telecommunications services with data security protection they paid for and the telecommunications services they received.

153. Had Defendant disclosed that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased telecommunications services from Defendant.

154. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their telecommunications services, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

155. Plaintiff and Class Members are entitled to compensatory and consequential

damages suffered as a result of the Data Breach.

156. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; (iii) verify the adequacy of security measures implemented by Defendant's third-party processors of AT&T's Private Information; and (iv) provide adequate credit and identity monitoring to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

157. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-114 as if fully set forth herein. Plaintiff brings this claim individually and on behalf of the Class Members.

158. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

159. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

160. The amount Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

161. Under the principles of equity and good conscience, Defendant should not be

permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

162. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

163. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

164. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to Defendant's services.

165. Plaintiff and Class Members have no adequate remedy at law.

166. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result

of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

167. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

168. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendant to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Defendant to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: April 1, 2024

Respectfully submitted,

/s/ Bruce W. Steckler
Bruce W. Steckler
Texas Bar I.D. 00785039
STECKLER WAYNE & LOVE PLLC
12720 Hillcrest Road, Suite 1045
Dallas, TX 75230
Telephone: (972) 387-4040
Facsimile: (972) 387-4041
bruce@swclaw.com

Jean S. Martin*
Francesca K. Burne*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 222-2434
jeanmartin@forthepeople.com
fburne@forthepeople.com

**pro hac vice to be filed*

Attorneys for Plaintiff and the Proposed Class